

⑫ 公開特許公報(A) 平3-185586

⑬ Int.Cl.³

識別記号

庁内整理番号

⑭ 公開 平成3年(1991)8月13日

G 06 K 17/00
G 07 F 7/12

T

6711-5B

8208-3E G 07 F 7/08

C

審査請求 未請求 請求項の数 3 (全6頁)

⑮ 発明の名称 ICカードの認証方法

⑯ 特 願 平1-325663

⑰ 出 願 平1(1989)12月14日

⑱ 発 明 者 吉 田 英 世

東京都新宿区榎町7番地 大日本印刷株式会社内

⑲ 発 明 者 若 松 雅 樹

東京都新宿区榎町7番地 大日本印刷株式会社内

⑳ 出 願 人 大日本印刷株式会社

東京都新宿区市谷加賀町1丁目1番1号

㉑ 代 理 人 弁理士 志 村 浩

明 細 書

1. 発明の名称

ICカードの認証方法

2. 特許請求の範囲

(1) ICカード内に、複数組の認証データとこの認証データの優先順位とを登録しておき、外部の端末機に用意された複数組の認証データに対して、前記登録した複数組の認証データを前記登録した優先順位で照合するICカードの認証方法において、

外部の端末機から前記優先順位の登録を更新しうるようにしたことを特徴とするICカードの認証方法。

(2) ICカード内に、複数組の認証データとこの認証データの優先順位とを登録しておき、外部の端末機に用意された複数組の認証データに対して、前記登録した複数組の認証データを前記登録した優先順位で照合するICカードの認証方法

において、

ICカード内に、個々のICカードに固有な識別データと、この識別データを利用して暗号データをデコードするアルゴリズムと、を記憶させ、外部の端末機から暗号データが与えられたときに、前記アルゴリズムに基づいてこの暗号データをデコードし、このデコード結果に基づいて前記優先順位の登録を新たなものに更新することを特徴とするICカードの認証方法。

(3) 請求項2に記載のICカードの認証方法において、

認証データの組数 n と同じ桁数 n の暗号データを用い、

識別データを構成する各桁を、 n 列複数行の行列に配し、各列ごとに論理演算を行い n 個の値を求め、この n 個の値のそれぞれと前記暗号データの各桁のそれぞれとの間で論理演算を行い前記 n 個の値を更新し、この n 個の更新値の大きさの順に基づいて新たな優先順位を決定することを特徴とするICカードの認証方法。

3. 発明の詳細な説明

(産業上の利用分野)

本発明はICカードの認証方法、特に、複数組の認証データとこの認証データの優先順位とをICカードに登録しておくICカードの認証方法に関する。

(従来技術)

磁気カードに代わる媒体として、ICカードの普及が期待されているが、ICカードの用途が広がれば広がるほど、セキュリティの重要性が増してくる。このため、ICカードを用いる場合には、その都度、認証を行うシステムが不可欠となる。

通常の認証方法としては、ICカード内の特定のメモリエリアに、認証データを登録しておき、ユーザーが端末機に与えた認証データと、ICカード内に登録された認証データとを比較する方法が行われている。また、更にセキュリティを向上させる方法として、たとえば、特開昭62-190583号公報には、ICカード内に、複数組の認証データを登録しておき、この複数組の認証デ

ータを種々のケースに応じて種々の優先順位で読出して照合する方法が開示されている。

(発明が解決しようとする課題)

上述の複数組の認証データを用いる方法では、単一の認証データを用いる方法に比べてセキュリティはかなり向上することになる。しかしながら、ユーザーは各ケースごとに認証データの人力を異なる順序で行う必要があり、操作性が悪くなるという問題がある。たとえば、前述の公報に実施例として記載された方法では、ICカードをアクセスしたときの時刻に応じて10とおりの優先順位を定めているが、ユーザーはそのときの時刻によって、認証データの人力順序を変えねばならず、非常に不便である。また、他人に認証手順を知られた場合、その認証手順が有効になる場合が1/10の確率で発生し、セキュリティの面でも問題がある。

そこで本発明は、操作性が良く、しかも高度なセキュリティを確保することのできるICカードの認証方法を提供することを目的とする。

(課題を解決するための手段)

(1) 本願第1の発明は、ICカード内に、複数組の認証データとこの認証データの優先順位とを登録しておき、外部の端末機に用意された複数組の認証データに対して、登録した複数組の認証データを登録した優先順位で照合するICカードの認証方法において、

外部の端末機から優先順位の登録を更新しうるようにしたものである。

(2) 本願第2の発明は、ICカード内に、複数組の認証データとこの認証データの優先順位とを登録しておき、外部の端末機に用意された複数組の認証データに対して、登録した複数組の認証データを登録した優先順位で照合するICカードの認証方法において、

ICカード内に、個々のICカードに固有な識別データと、この識別データを利用して暗号データをデコードするアルゴリズムと、を記憶させ、

外部の端末機から暗号データが与えられたときに、記憶しているアルゴリズムに基づいてこの暗

号データをデコードし、このデコード結果に基づいて優先順位の登録を新たなものに更新するようにしたものである。

(3) 本願第3の発明は、上述の第2の発明において、

認証データの組数 n と同じ桁数 n の暗号データを用い、

識別データを構成する各桁を、 n 列複数行の行列に配し、各列ごとに論理演算を行い n 個の値を求め、この n 個の値のそれぞれと暗号データの各桁のそれぞれとの間で論理演算を行い n 個の値を更新し、この n 個の更新値の大きさの順に基づいて新たな優先順位を決定するようにしたものである。

(作用)

(1) 本願第1の発明によれば、外部の端末機から優先順位の登録を更新することができる。したがって、他人に照合手順を知られたとしても、優先順位を変えてしまえば、もはや他人の不正なアクセスを受けることがなく、セキュリティが向

上する。また優先順位を変更する操作を行わない限り、同じ照合手順でアクセスできるため、操作性も良好である。

(2) 本願第2の発明によれば、優先順位の登録更新操作を行う場合、新たな優先順位を示す順位データは、そのままではなく暗号データの形式で端末機からICカードへと伝えられる。したがって、セキュリティ性がより向上する。

(3) 本願第3の発明によれば、ICカード固有の識別データに基づいて生成された行列と、与えられた暗号データと、に基づいて優先順位が決定される。したがって、セキュリティ性の高い更新作業が可能になる。

(実施例)

以下、本発明を図示する実施例に基づいて説明する。第1図は本発明の一実施例に係る認証方法を利用したICカードのアクセス手順を示す流れ図である。この手順について詳述する前に、ICカード内のデータ構成について簡単に説明しておく。第2図は、端末機10にICカード20を接

触例を示すものであり、この例によれば、認証データ②④①③の順序で照合が行われることになる。

デコードアルゴリズム領域24

端末機10から与えられた暗号データをデコードするためのアルゴリズムが格納される。具体的には、デコードのためのプログラムが格納されることになる。

カード番号領域25

各ICカードを識別するための固有のデータであるカード番号が格納される。この例では、たとえば、第5図に示すような18桁(本明細書では、一連のデータを構成する1データ単位を1桁と呼ぶことにする。この例では1バイトのデータ単位を1桁と呼んでいる)のデータからなるカード番号が格納されている。

ユーザデータ領域26

ICカードが記憶すべき本来のデータであるユーザデータが格納される。

なお、ICカードは、上述の各領域を有するメモリの他に、CPUなどのプロセッシングユニッ

統した状態を示すブロック図である。端末機10とICカード20の間では、図の矢印に示すようにデータがやりとりされる。ICカード20内には、種々のデータを格納するため、次の各領域が設けられている。

ディレクトリ領域21

他の各領域をアクセスするためのアドレス値などのディレクトリ情報が格納される。

認証データ領域22

複数組の認証データが格納される。ここで説明する例では、第3図に示すような4組の認証データ(いずれも16進データで示してある)を用いている。

順位データ領域23

複数組の認証データの優先順位を示す順位データが格納される。各認証データは、この優先順位にしたがって照合されることになる。この例では、前述のように4組の認証データが用いられているので、順位データはこの4組についての照合順位を示すものとなる。第4図は、この順位データの

トを附えているが、第2図には示されていない。

それでは、第1図の流れ図を参照して、この実施例のICカードのアクセス手順を説明する。はじめに、ユーザがICカード用のリーダ/ライタ装置にICカードを挿入すると、ステップS1の準備処理が行われる。この準備処理は、端末機10とICカード20の間でデータのやりとりを行うための準備を行う処理であり、たとえば、端末機10からICカード20に対してRESET信号を与えると、これに応じてICカード20から端末機10へANSWER TO RESET信号が返されることになる。

準備処理が完了すると、ステップS2において端末機10からICカード20へのコマンド入力を持つ状態となる。このコマンドは、認証コマンド、一般コマンド、順位変更コマンド、の3種類に分類され、コマンドの種類によってICカード20内の処理が異なる。

認証コマンドは、このICカードの持ち主が正當なユーザであるか否かを認証する作業を行うた

めのコマンドであり、通常は、ユーザデータをアクセスする前にこのコマンドが実施される。端末機10からこの認証コマンドが与えられると、ICカード20内において、ステップS3に示すように、認証データ領域22から認証データの読出しが行われる。読出された認証データは、順位データ領域23内の順位データに示す優先順位の順にしたがって、ユーザが端末機10に入力した認証データと一致するかが判定される(ステップS4)。この実施例の場合、第3図に示す4組の認証データが読み出され、第4図に示す順位、すなわち、認証データ②④①③の順序で照合が行われることになる。別言すれば、ユーザが端末機10に対して、認証データ②④①③の順で入力したときにのみ、両者は一致することになる。一致した場合には、ステップS5において照合フラグが1にセットされる。この照合フラグは、照合結果が一致した場合に1となり、不一致の場合あるいは認証作業がまだ行われていない場合には0となる。更にステップS6において正常ステータスがセッ

われた場合にはステップS11において正常ステータスがセットされる。また、ステップS8において、照合フラグが0であった場合、あるいはステップS10において異常発生と判断された場合には、ステップS12においてエラーステータスがセットされる。このように、認証コマンドを行い、照合フラグが1にセットされない限り、ステップS9のコマンド処理を行うことはできない。別言すれば、ユーザが正しい認証データを正しい優先順位で入力しない限り、ユーザデータをアクセスすることはできない。

順位変更コマンドは、本願発明の特徴となる処理を行うためのコマンドである。このコマンドの目的は、順位データ領域23内の順位データを変更することである。これはたとえば、ユーザが他人に認証データの入力操作を知られてしまったような場合に有効である。順位データを変更してしまえば、他人の知っている入力操作では、認証データの優先順位が異なるため、照合一致が不可能になり、セキュリティを向上させることができる。

トされる。一方、ステップS4において不一致であった場合には、ステップS7においてエラーステータスがセットされる。したがって、この場合は照合フラグは0のままとなる。以上が認証コマンドに対する処理手順である。

一般コマンドは、このICカードに対する本来のアクセス用コマンドである。たとえば、ユーザデータを端末機10側に読み出したり、ユーザデータを書き替えたりするコマンドなどが、この一般コマンドとなる。ICカード20は、端末機10からこの一般コマンドが与えられると、はじめにステップS8において照合フラグのチェックを行う。そして、照合フラグが1であれば、すなわち、既に認証コマンドに対する処理が行われ照合結果が一致した場合には、ステップS9へと進む。このステップS9では、与えられた一般コマンドに対する処理が行われる。たとえば、ユーザデータの読み出しや書き替えといった処理が実際に行われる。そして、ステップS10においてこの処理が正常に行われたか否かが判断され、正常に行

第4図に示す例では、現在の順位データは「2413」である。いま、この順位データを「3412」に変更する場合を例として説明する。はじめに、端末機10から、新たな順位データ「3412」に相当する暗号データをICカード20に与える。この暗号データは、ICカードのカード番号を用いて作成される。暗号の作成手順は、後述する暗号のデコード手順の逆であるから、ここでは説明を省略する。ICカード20は、暗号データを受け取ると、ステップS13においてこれをデコードする。デコードのためのアルゴリズムは、デコードアルゴリズム領域24内にプログラムとして記述されている。ここに述べる実施例では、次のようにしてデコードされる。まず、端末機10側から与えられた暗号データを、X1、X2、X3、X4とする。このアルゴリズムでは、暗号データの桁数は認証データの組数に一致する。したがって、この例の場合、4桁の暗号データが作成されている。はじめに、ICカード20は、自分自身に与えられた固有の識別データであるカー

ド番号を読み出す。ここで説明する例では、第5図に示す18桁（前述のように、この例では1バイトを1桁と呼ぶ）のカード番号が読み出される。このカード番号は、第6図に示すように、行列に配される。ここで、1行の列数は認証データの組数と一致させるようにする。すなわち、この例の場合は1行は4列で構成され、読み出したカード番号の最初の4桁は1行目、次の4桁は2行目、というように順に並べられてゆく。結局、この例の場合、5行4列の行列が形成されるが、カード番号は18桁しかないため、5行目の行列要素は2桁分不足する。そこで、これに対してパディング処理を施す。すなわち、不足分を何らかのデータで補うのである。どのようなデータで補うかは、予め決めておくことになるが、この実施例では、不足箇所には常に「20」なるデータを補うことにしている。こうして、第6図に示すような5行4列の行列が完成すると、各列ごとに論理演算を施す。たとえば、第1列目については、「A0、A4、A8、AC、B0」なる5桁のデータに対

して何らかの論理演算が施され、演算結果としてY1が得られる。この論理演算はどのようなものでもかまわないが、予め決めておかねばならない。たとえば、全データの論理和、論理積、排他的論理和などをとればよい。こうして、4列のデータすべてについて論理演算を行い、演算結果としてY1、Y2、Y3、Y4を得る。続いて、これら演算結果と端末機10から与えられた暗号データX1、X2、X3、X4との間で、それぞれ第7図に示すように所定の論理演算を行い、演算結果としてZ1、Z2、Z3、Z4を得る。これらを大きい順（または小さい順でもよい）に並べると、第8図に示すように、 $Z3 > Z4 > Z1 > Z2$ となったとする。これから、新たな順位データは「3412」と決定できる。このように、端末機10からICカード20へ暗号データを与えることにより、セキュリティをより向上させることができる。特に、端末機10とICカード20との間に何らかの回線が用いられている場合、この回線を介しての通信を盗聴された場合でも、順位デ

ータが漏洩することを防ぐことができる。

以上が暗号データのデコード手順の一例である。デコードが完了したら、ステップS14において、順位データの書き替えが行われる。すなわち、順位データ領域23に新たな順位データである「3412」が書き込まれる。そして、ステップS15において、この書き替え作業が正常に行われたかが判断され、正常であればステップS16で正常ステータスがセットされ、何らかの異常があればステップS17においてエラーステータスがセットされる。

以上、3種類のコマンド処理の手順を説明したが、各コマンド処理が終了すると、ステップS18において、全処理を終了するか否かが判断される。たとえば、全処理を終了すべきことを示す一般コマンドが与えられた場合には、ステップS18を経て全手順が終了する。終了しない場合は、再びステップS2のコマンド入力に戻る。このとき、正常ステータスかエラーステータスのいずれかがセットされているので、次のコマンド入力時

に端末機10側に何らかのメッセージを与えることができる。

なお、上述した実施例は本願発明の一実施態様を開示するものであり、本願発明はこの実施例のみに限定されるものではない。特に、暗号データのデコード方法は、これ以外にも種々の方法を採用することが可能である。また、ここでは1バイトの単位データを1桁のデータとして扱ったが、必ずしも1バイトを1桁とする必要はない。

〔発明の効果〕

(1) 本願第1の発明によれば、外部の端末機から優先順位の登録を更新することができるため、他人に照合手順を知られたとしても、優先順位を変えてしまえば、もはや他人の不正なアクセスを受けることがなく、セキュリティが向上する。また優先順位を変更する操作を行わない限り、同じ照合手順でアクセスできるため、操作性も良好である。

(2) 本願第2の発明によれば、優先順位の登録更新操作を行う場合、新たな優先順位を示す順

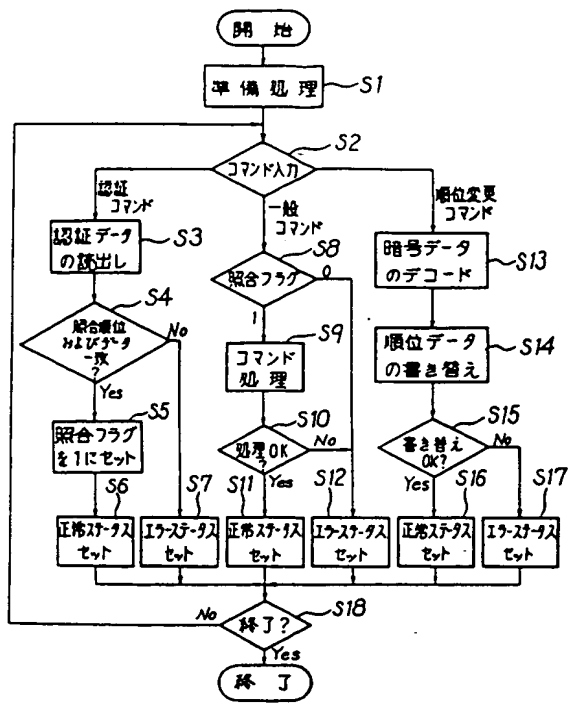
位データは、そのままではなく暗号データの形式で端末機からICカードへと伝えられるため、セキュリティ性がより向上する。

(3) 本願第3の発明によれば、ICカード固有の識別データに基づいて生成された行列と、与えられた暗号データと、に基づいて優先順位が決定されるため、セキュリティ性の高い更新作業が可能になる。

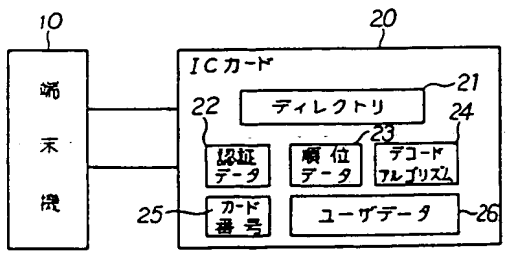
4. 図面の簡単な説明

第1図は本発明の一実施例に係る認証方法を利用したICカードのアクセス手順を示す流れ図、第2図は端末機10にICカード20を接続した状態を示すブロック図、第3図は認証データの一列を示す図、第4図は順位データの一列を示す図、第5図はカード番号データの一列を示す図、第6図～第8図は本発明に係る暗号データのデコード手順に必要な論理演算を示す図である。

出願人代理人 志 村 浩



第1図



第2図

22 認証データ領域

A6	87	B9	32	18	(認証データ①)
14	22	2A	6B	53	(認証データ②)
92	F8	EA	90	17	(認証データ③)
46	8D	5F	22	DB	(認証データ④)

第3図

23 順位データ領域

2	4	1	3
---	---	---	---

第4図

25 カード番号領域

A0	A1	A2	A3	A4	A5	A6	A7	A8
A9	AA	AB	AC	AD	AE	AF	B0	B1

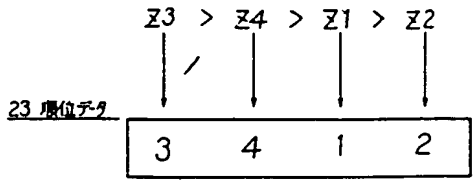
第5図

A0	A1	A2	A3
A4	A5	A6	A7
A8	A9	AA	AB
AC	AD	AE	AF
B0	B1	20	20
Y1	Y2	Y3	Y4

第6図

X1	X2	X3	X4
Y1	Y2	Y3	Y4
Z1	Z2	Z3	Z4

第7図



第8図

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.